SandBlast Mobile Integration with BlackBerry Dynamics and BlackBerry UEM

Administration Guide

Micha Burd

20 February 2018
Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Check Point Protect app for BlackBerry Dynamics | • Check Point Protect app with the BlackBerry Dynamics SDK integration.  
  • The app connects to the Sandblast Mobile Dashboard to provide device risk assessments.  
  • The app connects to Unified Endpoint Management (UEM) in order to lock BlackBerry containers. |
| Check Point SandBlast Mobile Cloud Solution | The Check Point SandBlast Mobile solution includes the following components:  
  • Behavioral Risk Engine  
  • Management Dashboard  
  • Gateways |
| BlackBerry UEM Server | • A Unified Endpoint Management server.  
  • UEM is used to configure and enforce secure container policy.  
  • The SandBlast Mobile solution uses the UEM policy to enforce device compliance. |
| BlackBerry Proxy | • A BlackBerry component that allows BlackBerry Dynamic apps to communicate with servers within the corporate network.  
  • The SandBlast Mobile app uses this service to communicate with Unified Endpoint Management. |
| BlackBerry NOC | • BlackBerry device communication component. |
The integration of SandBlast Mobile with BlackBerry Dynamics and BlackBerry Unified Endpoint Management does not require any incoming open ports on the corporate network firewall.

The SandBlast Mobile solution is based on the BlackBerry infrastructure for app provisioning, activation, and communication to Unified Endpoint Management.

**Provisioning and Mitigation Sequence Diagram**

1. UEM notifies the user to download and activate SandBlast Mobile for Blackberry.
2. The user downloads and activates the app. This is the same activation flow as any other BlackBerry Dynamics app.
3. SandBlast Mobile for the BlackBerry app is activated.
4. The BlackBerry SDK pulls the configuration data from UEM. The configuration includes:
   a. SandBlast Mobile Dashboard details (token, gateway name).
   b. The UEM host name.
   c. Credentials to lock BlackBerry Dynamic containers.
   d. The flag to use the lock API and not block (UEM server 12.7.2 does not support the block/unblock API).
   e. The flag to use the user’s email for the SandBlast Mobile device record.
5. The SandBlast Mobile app gets the dashboard details and automatically provisions the device on the SandBlast Mobile Dashboard.
6. The SandBlast Mobile app automatically registers the device to the SandBlast Mobile Dashboard.
7. The SandBlast Mobile app checks for device security risk changes.
8. If the device risk changes, the SandBlast Mobile app pulls the credentials details from the BlackBerry SDK object. The SandBlast Mobile app performs an API call to UEM to lock the BlackBerry Dynamic containers.

When the security risk changes to High, the container is locked. A lock event is not reversible using the API. The user will need a new activation key to open the locked container.
SandBlast Mobile Dashboard Configuration

Before you start reading this section, make sure you have:

1. A link to the SandBlast Mobile Dashboard.
2. SandBlast Mobile Dashboard admin user credentials.
3. The UEM username and password with permission to use the following Good Control SOAP APIs:
   * GetUser*
   * GetDevices*
   * EnforceContainerAction*

   These credentials will be used by the SandBlast Mobile app to interact with Unified Endpoint Management.

Step by step instructions to configure the SandBlast Mobile Dashboard:

1. Connect to the Dashboard, and sign in with admin credentials.
2. Go to the Devices tab, and verify there are no devices in the Dashboard.
3. Go to the Settings tab.
4. From the left navigation pane, click on Device Management section.

5. In Device Management Settings section, open the drop box, and select Good Dynamics.
6. Enter the applicable information in these fields:
   a) Host Name (without https://)
   b) User Name
   c) Password

   Turn off the “Import device owner email”, if the Dashboard should not use the device owner’s email for device records.

   Device records are created using device Mobile Device Management (MDM) ID.

7. Click Save and close the window.

8. Copy the configuration text. You will use it in the UEM app configuration.

Example:
UEM Configuration

Before you start reading this section, make sure you have:
1. Unified Endpoint Management admin user credentials.
2. The SandBlast Mobile configuration text from the previous section.

Step-by-step instructions to configure SandBlast Mobile app in the BlackBerry UEM:
This does not replace the UEM Administration Guide. If you need more configuration
details on the UEM settings, refer to the UEM Administration User Guide.

1. Log in to Unified Endpoint Management.
2. From the left navigation pane, select Apps.

3. In the right pane, click on Add an app.

4. Select Google Play, or App Store.
5. Search for “SandBlast Mobile for BlackBerry”, and add the app.
6. Open the app settings from the app screen.

Example:

7. In the **Server configuration payload** section, click **Add**.
8. Paste the configuration JSON, which was generated on the SandBlast Mobile Dashboard.
   
   Note - Refer to the **Appendix** for manual changes that need to be done in the JSON.
9. Check the box **“Allow BlackBerry Dynamics apps to use user certificates”**.
10. Assign the app to a Blackberry Dynamic profile.
    
    Make sure that SandBlast Mobile app is set as the authentication delegation.
11. Click **Save**.
12. Click **Policies and Profiles**.
13. Search for BlackBerry Dynamics connectivity profile.
    
    a. Edit the BlackBerry Dynamics connectivity profile.
    
    b. Click **Add Server**.
    
    c. Select the SandBlast Mobile app.
d. Click on the plus icon to add an app server.

e. In the **Server** field, enter the name of the Unified Endpoint Management server.

f. In the **Port** field, enter 18084.

g. In the **Priority** field, select Primary.

h. In the **Primary BlackBerry Proxy cluster** field, select First.

Example:

```
14. If the Unified Endpoint Management is set to work with a self-signed certificate, create a Certificate Authority (CA) certificate profile with the self-signed certificate.

15. Create a user group that includes:
   a. Users that will use the SandBlast Mobile app.
   b. The BlackBerry Dynamic profile created in Step 9.
   c. The BlackBerry connectivity profile created in Step 13.
   d. The CA certificate profile created in Step 14.
```
Install and Activate SandBlast Mobile App on a Device

Before you start reading this section, make sure you have the Unified Endpoint Management activation code for the SandBlast Mobile app.

**Step-by-step instructions to activate the SandBlast Mobile app:**
1. Download and install the app.
2. Launch the app and enter Unified Endpoint Management activation code.
3. Create container password.
4. After the app is activated, a scan process is initiated automatically.
5. If the device risk changes to High, all secure containers on the device are locked.
Appendix

Dashboard configuration text:

- Add the red lines manually after pasting the JSON file from the Dashboard.
- gcDomain is the AD domain of the admin user. If no AD is configured, use LOCAL.
- gcTenantId is the SRP ID of the UEM server. See the BlackBerry KB article 000004744 to learn how to locate it.
- useLockContainer is a Boolean value. For UEM server, set this value to true.

```json
{
    "token": "4539e9b00b8ee66a2146cf29c6d047552c17e83626796b3da4a766de17dc03f0",
    "gwHost": "gw.locsec.net",
    "gcUsername": "admin",
    "gcPassword": "XGQH/UFDB2GPR2QBUjKxw==",
    "gcDomain": "LOCAL",
    "gcTenantId": "S51620706",
    "useLockContainer": true,
    "gcEmailRegistration": true
}
```